CLAIMS

What is claimed is:

1. A secure processing system for a communication device comprising:

a host processor; and

a secure memory coupled to the host processor by a data bus, wherein the secure memory comprises:

a laser-scribed encryption key;

encryption logic circuitry for implementing a symmetric encryption algorithm using the laser-scribed encryption key;

a plurality of blocking gates coupling the encryption logic circuitry with the laser-scribed encryption key; and

a memory,

wherein sensitive data is encrypted by the encryption logic circuitry using the laser-scribed encryption key and stored as encrypted data in a data storage medium, and

wherein the encrypted data is decrypted by the encryption logic circuitry with the laser-scribed encryption key and transferred to the memory for use by the host processor.

2. The processing system as claimed in claim 1 wherein the memory is a zeroizable memory having a zeroizing input that causes the contents of the memory to be erased when a zeroize signal is received on the zeroizing input, and

wherein said zeroize signal is sent to the zeroizable memory by a system monitor upon the occurrence of one of a plurality of predetermined conditions.

3. The processing system as claimed in claim 1 wherein the host processor and secure memory are fabricated on an integrated circuit chip, and the encrypted data is stored in a non-volatile memory.

4. The processing system as claimed in claim 3 wherein the non-volatile memory includes a portion internal to the integrated circuit chip and a portion external to the integrated circuit chip, and wherein the encrypted data is stored on the portion internal to the integrated circuit chip when the portion internal is available.

5. The processing system as claimed in claim 1 wherein the blocking gates are comprised of logic gates and have a blocking control signal input preventing access to the laser-scribed encryption key by the encryption logic circuitry.

6. The processing system as claimed in claim 1 wherein the laser-scribed encryption key is stored in a one-time programmable memory element.

7. The processing system as claimed in claim 1 wherein the laser-scribed encryption key is stored in non-volatile memory selected from one of the group consisting of ROM, EEPROM, MRAM (Magnetoresistive RAM), battery backed RAM or DRAM and fast logic.

8. The processing system as claimed in claim 1 wherein the laser-scribed encryption key is generated by laser-scribing a semiconductor die during fabrication of the secure memory to create a plurality of fixed "ones" and "zeroes" which make up the laser-scribed encryption key, and

wherein the laser-scribed encryption key has a value that is randomly generated and is unique for each secure memory of a plurality of secure memories of different processing systems.

9. The processing system as claimed in claim 1 wherein the laser-scribed encryption key is generated by burning one-time programmable fuses on a semiconductor die to create a plurality of fixed "ones" and "zeroes" which make up the laser-scribed encryption key, and

wherein the laser-scribed encryption key has a value that is randomly generated and is unique for each secure memory of a plurality of secure memories of different processing systems.

10. The processing system as claimed in claim 1 wherein the symmetric encryption algorithm is a block cipher encryption algorithm.

11. The processing system as claimed in claim 1 wherein the host processor is coupled to an external memory having a secret key stored therein in encrypted form, the secret key being encrypted with the laser-scribed encryption key, and said secret key being used for secure communication between the communication device and other communication devices.

12. A secure communication device comprising:

a host processor;

a secure memory coupled to the host processor by a data bus, the secure memory including a laser-scribed encryption key; and

a non-secure memory coupled to host processor for storing encrypted data,

wherein sensitive data is encrypted within the secure memory using the laser-scribed encryption key and stored as encrypted data in the non-secure memory, and

wherein the encrypted data is decrypted within the secure memory using the laser-scribed encryption key and stored within the secure memory for use by the host processor.

13. The communication device as claimed in claim 12 wherein the non-secure memory has a secret key stored therein in encrypted form, the secret key being encrypted with the laser-scribed encryption key, and said secret key being used for secure communication between the communication device and other communication devices.

14. The communication device as claimed in claim 12 wherein the communication device is a data communication device, and wherein the secret key is a private key unique to a user of the communication device and is part of a public-private key pair, the private key being used for decrypting data sent to said user, and wherein prior to using said secret key, said secret key being decrypted by encryption logic of the secure memory using the laser-scribed encryption key and stored in unencrypted form in a zeroizable memory.

15. The communication device as claimed in claim 14 wherein the data communication device is adapted for transmitting data to another communication device, and wherein the secret key is further used to generate a digital signature associated with said data, said digital signature being transmitted along with said data.

16. The communication device as claimed in claim 12 wherein the communication device is a wireless communication device for communicating secured voice, and wherein the secret key is used for generating a common session key for communicating with another communication device,

and wherein prior to using said secret key, said secret key being decrypted by encryption logic of the secure memory using the laser-scribed encryption key and stored in unencrypted form in zeroizable memory.

17. The communication device as claimed in claim 12 wherein the secret key is one of a plurality of secret encryption keys stored in encrypted form in the non-secure memory, the plurality of secret keys being encrypted with the laser-scribed encryption key, and

wherein one of the secret keys of the plurality is selected for secure communication between the communication device and other communication device, and wherein a zeroizable memory is cleared after communication with the other communication device, and

wherein prior to using said selected secret key, said selected secret key is decrypted by the encryption logic using the laser-scribed encryption key and stored in unencrypted form in the zeroizable memory.

18. The communication device as claimed in claim 12 wherein the secure memory further comprises:

a plurality of blocking gates coupled to the laser-scribed encryption key;

encryption logic circuitry for implementing a symmetric encryption algorithm using the laser-scribed encryption key and coupled to the blocking gates; and

a zeroizable memory coupled to the encryption logic circuitry,

wherein sensitive data is encrypted by the encryption logic circuitry using the laser-scribed encryption key and stored as encrypted data in the non-secure memory, and

wherein the encrypted data is decrypted by the encryption logic circuitry with the laser-scribed encryption key and transferred to the zeroizable memory for use by the host processor.

19. A method of using secure information utilizing a secure communication device, the secure communication device comprising a host processor, a secure memory coupled to the host processor by a data bus, and a non-secure memory coupled to host processor for storing encrypted data, wherein the secure memory includes a laser-scribed encryption key stored therein, the method comprising the steps of:

encrypting sensitive data within the secure memory using the laser-scribed encryption key;

storing the encrypted sensitive data in the non-secure memory;

decrypting the encrypted sensitive data within the secure memory using the laser-scribed encryption key; and

storing the decrypted sensitive data within the secure memory for use by the host processor.

20. The method as claimed in claim 19 wherein the secure memory includes blocking gates coupled between encryption logic circuitry and the laser-scribed encryption key, and a zeroizable memory coupled to the encryption logic circuitry, and wherein the storing step comprises storing the decrypted sensitive data within the zeroizable memory, and wherein the method further comprises the steps of:

disabling the blocking gates during the encrypting and decrypting steps; and

zeroizing the zeroizable memory after the host processor is through using the decrypted sensitive data stored in the zeroizable memory.

21. The method as claimed in claim 20 further comprising the step of enabling the blocking gates preventing the encryption logic circuitry from accessing the laser scribed encryption key, the step of enabling being performed upon completion of the decrypting step.